ilmedia

TECHNISCHE UNIVERSITÄT
ILMENAU

Daniel Fischer und Bernd Markscheffel:

The German wireless LAN security survey 2009 – How security measures are used in companies and federal authorities?

Zuerst erschienen in:
International journal for infonomics (IJI) / Infonomics Society. - [S.l.] : Infonomics Society, ISSN 1742 4712, Vol. 3.2010, 2.
S. 278 - 284

The German Wireless LAN Security Survey 2009 - How Security Measures are used in Companies and Federal Authorities?

D. Fischer and B. Markscheffel
Ilmenau University of Technology
{daniel.fischer|bernd.markscheffel}@tu-ilmenau.de

Abstract

The paper presents a couple of findings of a study in wireless LAN security (WLAN) in German companies and federal authorities. The study was conducted in spring 2009. On the basis of a directory of security measures we formulate hypotheses derived from several studies in WLAN security. We analyze how the situation in Germany fits these assumptions. Degree of familiarity, frequency of use and reasons for not using wireless LAN security measures are being investigated. Furthermore, we discuss correlations between companies' characteristics and the use of security measures.

1 Introduction

The integration of computer systems into a comprehensive network is one of the key elements for companies and federal authorities' effective and flexible work. Wireless solutions are increasing the flexibility and mobility here. Wireless local area networks (WLANs) are an important technology in this area. The main focus of criticism, regarding the use of WLANs, is their lack of security [1], [2], [3], [4]. For example, a Europe-wide study from Motorola Research shows that more than half of the observed 400 companies have insufficiently secured WLANs [5]. On the one hand there exist a lot of security measures, but on the other hand there is a great lack in the appropriate use of them. In this case potential attackers can easily gain access to mission critical data or crash security relevant applications.

After a first survey concerning the status quo in WLAN security in 2006 [6], [7] we restarted the investigation in spring 2009. In this paper we summarize selected results of this explorative study in order to find answers to a plenty of questions like:

- How popular and known are security measures for WLANs?
- Which security measures are used by companies and federal authorities, which are not and why?
- Are there correlations between companies' characteristics and the use of security measures?

In the next section of the paper we show how the empirical study was prepared and conducted and we present our directory of WLAN security measures. In the third section we describe and discuss the results of the survey. Finally we summarize our results and close with an outlook for future research questions.

2 Methodology

Main objective of our survey is a state of the art report of WLAN security in German companies and federal authorities. To specify the above mentioned questions we formulated hypotheses dealing with the use of WLAN security measures, reasons for non-use and several other problems. These hypotheses were derived from various studies in WLAN security [1], [2], [3], [4], [5], [8], [9], [10], [11], and combined with our results from the previous study [6], [7] to serve as basis for the online questionnaire [12].

The questionnaire is divided in three sections. The first part is devoted to the characteristics of the respondents. In the second part we are gathering information dealing with the respondents WLAN infrastructure. The third and main part contains the questions concerning the WLAN security measures. Basis of this part is a directory of categorized WLAN security measures [13]. We have compiled a set of 53 security measures which were classified into the following four main classes:

i. organizational measures before use
ii. organizational measures during operation
iii. hardware measures
iv. software measures

The directory is a result of an analysis of several standard publications in the WLAN security field e.g.: information sheets concerning WLAN security of the German Federal Office for Information Security BSI [4], [8], [14], the security specification of the IEEE standard family 802.11 [11], the ISO/IEC 27000 standard family [15], [16] and other publications [17], [18]. Table 1 shows this compilation.

Copyright © 2010, Infonomics Society

Table 1. Directory of WLAN security measures

Organizational measures before use
Defining a security concept for the WLAN infrastructure
01: Define the needs, objectives and purpose of the WLAN infrastructure
02: Define requirements for security objectives
03: Assess the protection requirements and performing a risk analysis
04: Create WLAN policy
Rollout planning
05: Define the work place of WLAN infrastructure
06: Regard environmental factors (sources of interference, structural environment)
07: Perform measurement planning (detection of signal strength)
08: Choose suitable antennas and the position for the access points that provides optimum WLAN coverage
09: Configure the channel allocation without overlapping (max. 3 parallel channels at 802.11b, g and max. 8 parallel channel at 802.11a)
10: Check the WLAN operation with the help of network scans and log-files inspection
Other organizational measures before WLAN installation
11: Perform tests prior to the actual WLAN installation
12: Develop emergency strategies to handle sudden security threats
13: Define access passwords for WLAN and LAN independently
14: Train and sensitize the users
15: Train administrators
16: Create documentation of WLAN infrastructure
Organizational measures during operation
17: Examine the compliance with data security regulations periodically
18: Monitor the WLAN with the help of network scans and log-files inspection regularly
19: Monitor the use of security measures under urgent security threats
20: Limit access to the access points to authorized staff
21: Don't administrate the access points via WLAN interface respectively unsecure administration accounts
22: Check the WLAN policy regularly
23: Check accessibility and integrity of the access points on-site regularly
24: Check configuration of the access points and WLAN equipment regularly
25: Update the documentation of the WLAN infrastructure regularly

Hardware measures
26: Choose suitable WLAN equipment (signal equipment: e.g. OFDM/DSSS) and standards (IEEE 802.11g, etc.)
27: Use a centralized management component for administration and monitoring of the WLAN (e.g. Wireless Switch)
28: Power on the WLAN-equipment only while using, or use time-controlled activation
29: Achieve signal encapsulation trough structural measures (e.g. shielding)
30: Lend registered WLAN cards and exchange WLAN cards regularly
Software measures
Configuration and administration of WLAN devices
31: Change factory presets
32: Deactivate the ad-hoc-networking ability
33: Use own (secure) SSID
34: Disable SSID broadcasting
35: Maximise beacon interval
36: Disable DHCP at the access points
37: Secure the connection between central authentication server (e.g. RADIUS) and access points
38: Use only one WLAN standard, instead more parallel (e.g. 'G-only' or 'B-only')
39: Use block-intra-BSS-traffic in public areas
Apply authentication mechanisms
40: Authentication via MAC-address filter mechanisms
41: Open system authentication
42: Pre-shared key authentication
43: 802.1X/EAP authentication
Apply encryption mechanisms
44: WEP encryption
45: WPA encryption
46: WPA2 or IEEE 802.11i encryption
47: VPN/IPsec (encryption on IP level)
Other software-technical measures
48: Separate WLAN and wired networks on the network level (e.g. via packet filter, VPN or VLAN)
49: Maintain software updates at the access points and WLAN devices regularly
50: Install a personal firewall at the WLAN-device
51: Change WLAN key at access points regularly
52: Use intrusion detection systems to monitor the WLAN
53: Restrict file and resource sharing on devices, which are connected with the WLAN

Copyright © 2010, Infonomics Society

We have asked the audience for each security measure

- if the specific measure is known
- and when *yes*, if it is used,
- if known but *not used*, we asked why not?

For the questioning we used a web-based tool (http://www.datenassistent.de) and as an alternative we made an offline-version (printable PDF-file) available.

After some pre-tests with hand-picked enterprises we carried out the investigation in cooperation with TeleTrusT Germany e.V. and the IT company NetSys.IT during the period April to June 2009.

As sample we selected enterprises and federal authorities which may have a relative high number of WLAN installations and therefore a high level of interest in solving WLAN security problems. So, we invited via e-Mail

i. the 110 enterprises of the main German stock indices (DAX, MDAX, TecDAX),
ii. the 94 members of the TeleTrusT Germany e.V. and
iii. approx. 100 security administrators of the federal administrations in Germany.

In addition to that we published a call for participation in two German key journals for information security (DuD - circulation 2.300 and <kes> - circulation 8.800) and in several information security or IT focused internet portals (e.g. http://www.heise.de/security, http://www.securitymanager.de, http://www.sicher-im-netz.de).

3. Results

210 enterprises and federal authorities took part in the survey. 115 of the 210 participants are using WLAN infrastructures, 12 more are planning the use. So we have 127 participants, 80 of them answered the questionnaire part, dealing with the security measures, completely and they are becoming the universe of research (n_c=80) for the upcoming analysis. The structure of the survey participants is as follows (The participants had the choice to state ‚no entry' for each question, that's why the sum of the individual values is sometimes not 100%):

i. concerning branch
   - 73.8% enterprises,
     - 32.5% service enterprises
     - 18.8% industrial enterprises
     - 16.3% ICT companies
     - 6.3% commercial enterprises
   - 13.8% federal authorities

ii. concerning size
   - 32.5% large (>250 employees)
   - 13.8% medium (51-250 employees)
   - 12.5% small (10-50 employees)
   - 25.0% micro (<10 employees)

iii. concerning geographical distribution
   - 25.0% from North Rhine-Westphalia
   - 16.3% from Bavaria
   - 8.8% from Baden-Wuertemberg
   - 8.8% from Hesse
   - 8.8% from Thuringia
   - 5.0% from Saxony-Anhalt

iv. concerning the position of the participants within the institution
   - 63.8% member of IT department
   - 11.3% member of management
   - 3.8% member of non-IT departments

Our analysis is limited to methods of descriptive statistics. In the following sections we discuss selected hypotheses using frequencies, arithmetic means and variances. We refrain from significance tests, because our sample is not a random one.

3.1. Use of WLAN security measures and reasons for non-use

Hypothesis 1: Companies and federal authorities prefer technical measures to protect their WLAN infrastructure more than organizational measures!

The protection of a WLAN infrastructure requires both organizational and technical measures. But, compared to technical measures organizational measures often require much more effort. That's why we assumed the preference of technical measures.

But it failed; we found that the participants use more (44.0%) organizational measures than technical measures (25.6%). This is illustrated in table 2, which shows in percentage terms the frequency of use of security measures. Within the top ten list we found only two technical measures.

Table 2. Tops/flops of used WLAN security measures

Measure/ Description	Class	Frequency of use
05: Define the work place of WLAN infrastructure	organizational	67.5%
01: Define the needs, objectives and purpose of the WLAN infrastructure	organizational	62.5%
31: Change factory presets	technical	61.3%
02: Define requirements for security objectives	organizational	58.8%
21: Don't administrate the access points via WLAN interface respectively unsecure administration accounts	organizational	56.3%
15: Train administrators	organizational	55.0%
06: Regard environmental factors (sources of interference, structural environment)	organizational	53.8%

Copyright © 2010, Infonomics Society

13: Define access passwords for WLAN and LAN independently	organizational	53.8%
16: Create documentation of WLAN infrastructure	organizational	52.5%
33: Use own (secure) SSID	technical	50.0%
40: Authentication via MAC-address filter mechanisms	technical	18.8%
43: 802.1X/EAP authentication	technical	18.8%
35: Maximise beacon interval	technical	13.8%
51: Change WLAN key at access points regularly	technical	13.8%
52: Use intrusion detection systems to monitor the WLAN	technical	13.8%
29: Achieve signal encapsulation trough structural measures (e.g. shielding)	technical	12.5%
41: Open system authentication	technical	10.0%
39: Use block-intra-BSS-traffic in public areas	technical	6.3%
30: Lend registered WLAN cards and exchange WLAN cards regularly	technical	5.0%
44: WEP encryption	technical	5.0%

Hypothesis 2: Main reasons for the non-use of security measures are lack of knowledge, high effort of implementation and use, and minor effects!

Manuals, guidebooks and papers often concentrate on few, selected measures [2], [3], [4], [18]. Often the focus is on the IEEE 802.11 standard family. A lot of organizational and technical aspects are too short or mentioned as a side issue. This is the reason for our assumption that most of the participants have a lack of knowledge concerning the majority of WLAN security measures and therefore do not make use of it. We expected also that another main reason for the non-use is the high effort of implementation and use and minor effects.

The results of our investigation showed that the participants knew only 55.4% of 53 measures mentioned in the questionnaire. 44.6% of the measures are unknown. Thus, lack of knowledge is the main reason for non-use.

We could observe the greatest lack of knowledge especially in the software- and hardware measures classes (see Figure 1). Furthermore we can see that the participants did not use all the measures they knew. Quit obvious is the difference between known and used security measures also in the above mentioned classes.

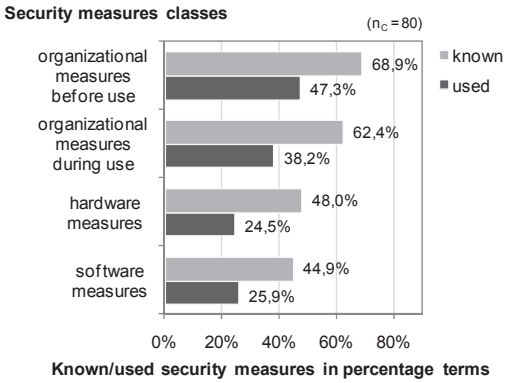

Figure 1. Degree of familiarity and frequency of use according to measure classes

This mismatch becomes more evident when we analyze individual measures (see figure 2): e.g. only 5.0% of the participants using WEP encoding even though they knew it.

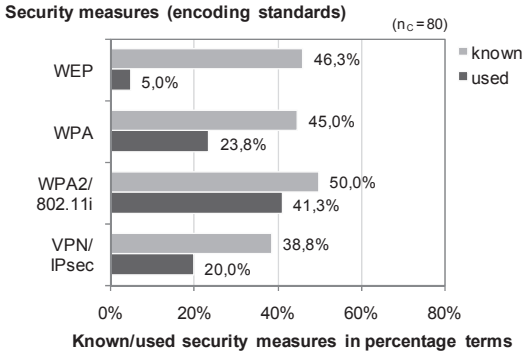

Figure 2. Degree of familiarity and frequency of use of encoding standards

So we must identify other reasons, beside the lack of knowledge, which are responsible for the non-use of specific measures. The analysis of the explained reasons of the participants has emphasized the second part of our hypothesis. 27.4% of participants questioned said that the high effort of implementation and use is the reason for non-use, 19.2% mentioned the minor effects. 43.1% are already planning the use of security measure, so we might see a significant increase in the use of security measures in the near future.

We have also analyzed the reasons for non-use for specific security measures and found that for hardware-technical measures the high effort of implementation and use is the main reason.

3.2. Correlations between company-specific characteristics and WLAN security measures

Hypothesis 3: Information and communication technology (ICT) companies using more security measures compared to other branches and federal authorities!

Copyright © 2010, Infonomics Society

ICT companies have a lot of experience and knowledge in the field of computer based communication and information management. That's why we assume a greater sensibility for security questions and therefore a more frequent use of security measures than in other branches.

But our analysis showed that federal authorities (47.4%) and industrial enterprises (45.6%) use more of the 53 in the questionnaire mentioned security measures than ICT companies (44.5%). The same conclusion can be drawn from figure 3, which shows the frequency of use, classified in the above described classes. In none of the classes ICT companies reached the highest frequency of use.

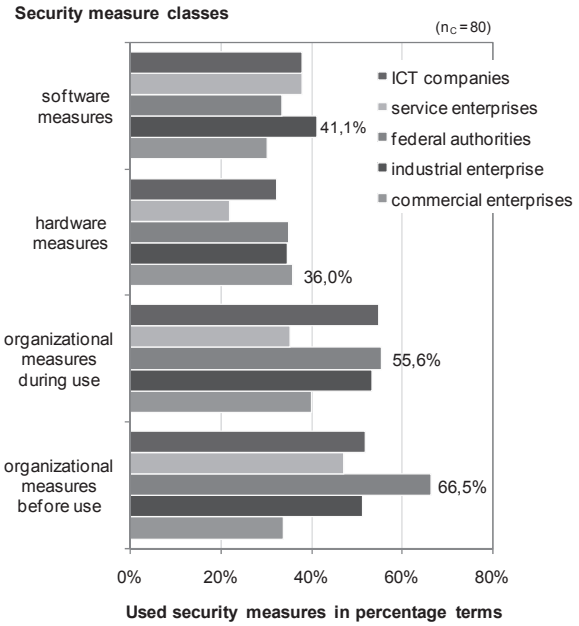

Figure 3. Frequency of use depending on branches and measure classes

Hypothesis 4: Enterprises and federal authorities with an IT security management use more security measures than institutions without a security division.

The institutionalization of IT security management acts as an enabler for the coordinated planning, implementation and monitoring of security of IT infrastructure as a whole. Main objective is to guarantee a desired security level permanently. But an ongoing development of IT security know-how is a necessary prerequisite. 36 of 80 participants (45.0%) have such a division or department. We assumed that these institutions use more security measures than institutions without an IT security division.

We found that the institutions with an IT security management use average 45.5% of our mentioned security measures. Institutions without such an IT security department use only 32.0%. An extremely strong correlation was found between the presence of IT security management and organizational measures (see figure 4).

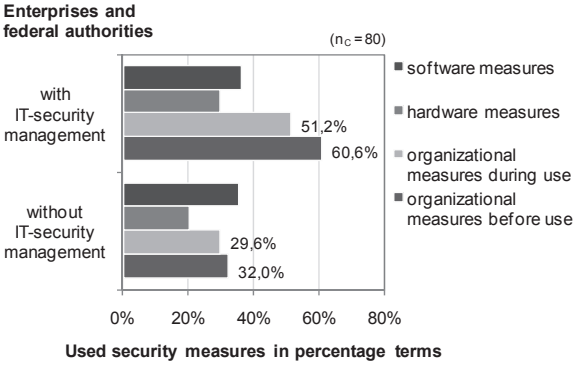

Figure 4. Frequency of use of security measures depending on the existence of an IT security management division

Hypothesis 5: The bigger an institution is the more it applies WLAN security measures.

Large enterprises and federal authorities have normally one or more IT departments and therefore a higher number of IT experts compared to smaller institutions. That's why we assumed that the more know-how in the field of IT security is reflected in the number of used WLAN security measures.

Figure 5 shows that the above expressed assumption cannot be verified. The degree of familiarity of WLAN security measures is the highest in large enterprise (73.1%) but this not considerably more than in smaller institutions (72.4%). On the other hand, if we consider the frequency of use we found the small institutions leading the list.

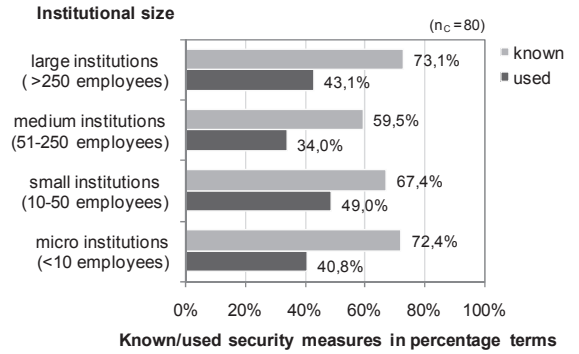

Figure 5. Degree of familiarity and frequency of use of security measures depending on the institutional size

But if we take a closer look at individual security measures we find correlations between institutional

Copyright © 2010, Infonomics Society

size and the use of security measures. We can identify measures which are more often used in large institutions as well as measures which are more often used by small and micro institutions.

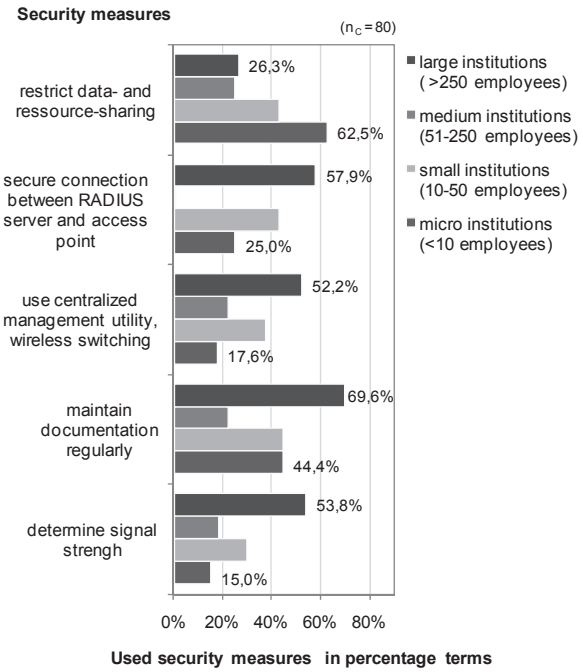

Figure 6. Frequency of use of special security measures depending on the institutional size

4. Conclusion

Our investigation allowed us to derive detailed statements concerning the degree of familiarity and frequency of use and the main reasons for non-use of WLAN security measures in German enterprises and federal authorities. The basis was a directory, developed by us, which consists of 53 WLAN specific security measures. We could also derive correlations between the use of these measures and institutional characteristics.

However, we must consider critically, that: a) the basis for our investigation, the questioned participants, was not a random sample, so we cannot make general statements. b) we have not considered the difference in effectiveness of the several security measures. Our statements are solely based on the number of security measures that the participants have used.

But this investigation can be seen as a starting point for future research. In the next step we plan to do cluster analysis in order to identify typical measurement clusters for the protection of WLAN infrastructure. Another interesting field of investigation is to compare the actual results with the findings of our study from 2006 to identify changes in using WLAN security measure in German enterprises and federal authorities. We plan further, comparable surveys. Also a European-wide investigation is conceivable. Regular repetitions would allow us to identify trends in the WLAN security. Another interesting field of investigation is to develop our measure directory further. In particular, the evaluation of the quality or effectiveness of the several security measures is of great importance. This would enable us to assess WLAN security even better.

The main title (on the first page) should begin 1-3/8 inches (3.49 cm) from the top edge of the page, centered, and in Times 14-point, boldface type. Capitalize the first letter of nouns, pronouns, verbs, adjectives, and adverbs; do not capitalize articles, coordinate conjunctions, or prepositions (unless the title begins with such a word). Leave two 12-point blank lines after the title.

5. References

[1] N. Borisov, I. Goldberg, D. Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11", in *Proceedings of the 7th annual international conference on Mobile computing and networking*, Rom, 2001, pp. 180-189.

[2] RSA-Security Inc. (Ed.), *The Wireless Security Survey of San Francisco*, 03/2005, http://www.securitymanagement.com/library/rsa_wireless0606.pdf (Accessed 2006-04-05).

[3] RSA-Security Inc. (Ed.), *The Wireless Security Survey of London*, 7th Edition, 08/2008, http://www.rsa.com/solutions/wireless/survey/WLANLN_WP_1008.pdf (Accessed 2009-03-15).

[4] Federal Office for Information Security BSI (Ed.), *Drahtlose Kommunikationssysteme und ihre Sicherheitsaspekte*, Bonn, 2006, http://www.bsi.bund.de/literat/doc/drahtkom/drahtkom.pdf (Accessed 2009-04-10).

[5] Motorola Research, Vanson Bourne, *Reveals 64 percent of Companies Neglect WLAN Security*, 03/2009, http://mediacenter.motorola.com/content/Detail.aspx?ReleaseID=10985&NewsAreaID=2 (Accessed 2009-04-15).

[6] D. Fischer, D. Stelzer, D. Kreyßel, *Verbreitung und Sicherheit von Wireless LAN-Infrastrukturen – eine empirische Untersuchung unter deutschen Unternehmen und Behörden*, Ilmenauer Beiträge zur Wirtschaftsinformatik Nr. 2006-03, Ilmenau, 2006.

[7] D. Fischer, D. Stelzer, „Eine empirische Untersuchung zur Verbreitung und Sicherheit von WLAN-Infrastrukturen", in C. Hochberger, R. Liskowsky (Eds.), *INFORMATIK 2006 Informatik für Menschen - Band 2*, Lecture Notes in Informatics (LNI), Bonn, 2006, pp. 523-529.

[8] Federal Office for Information Security BSI (Ed.), *Technische Richtlinie Sicheres WLAN (TR-S-WLAN)*, Bonn, 2005.

Copyright © 2010, Infonomics Society

[9] Detecon (Ed.), *Trendletter Public WLAN – Hot Spot Report*, 12/2003, http://www.detecon.com/de/publikatio n en/studienbuecher_detail.php?pub_id=75 (Accessed 2006-05-30).

[10] Wick Hill (Ed.), *Wireless Networking in Deutschland*, 10/2004, http://www.nexthop.de/de/clients/wickhill/press/ wh20040915.pdf (Accessed 2006-05-30).

[11] Institute of Electrical and Electronics Engineers IEEE - The Working Group for WLAN Standards (Ed.), *Wireless LANs Standards (802.11)*, 02/2009, http:// grouper.ieee.org/ groups/802/11/ (Accessed 2009-02-15).

[12] D. Fischer (Ed.), *Studie zur Sicherheit von Wireless LAN Infrastrukturen 2009 (Questionnaire)*, 2009, http:// www.wlan-sec.de/Fragebogen2009.pdf (Accessed 2009-08-25).

[13] D. Fischer (Ed.), *Directory of WLAN-security measures 2009*, 09/2009, http://www.wlan-sec.de/WLAN security-measures_2009.pdf (Accessed 2009-08-30).

[14] Federal Office for Information Security BSI (Ed.), *Sichere Nutzung von WLAN - BSI-Leitlinie zur Internet-Sicherheit (ISi-WLAN)*, Bonn, 2009.

[15] International Organization for Standardization ISO (Ed.), *ISO/IEC 27001:2005: Information technology, Security techniques, Information security management systems, Requirements*, 2008-10-15, http://www.iso.org/ iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnu mber=42103 (Accessed 2009-02-21).

[16] International Organization for Standardization ISO (Ed.), *ISO/IEC 27002:2005: Information technology, Security techniques, Code of practice for information security management*, 2008-04-22, http://www.iso.org/ iso/catalogue_detail?csnumber=50297 (Accessed 2009-02-21).

[17] S. Fluhrer, I. Mantin, A. Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4", in *Lecture Notes in Computer Science,* Vol. 2259, 2001, pp. 1-24.

[18] H. Kopp, *Einsatz von WLAN in Unternehmen – Leitfaden*, Electronic Commerce Center Mecklenburg-Vorpommern, 9/2004, http://www.eccom.de/wDeutsch/do kumente/leitfaeden/Leitfaden_wlan.pdf?navid=16 (Accessed 2009-02-13).

Copyright © 2010, Infonomics Society